

10-2-00

A
10925 U.S. PTO
09/675467
09/28/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship..... Blinn et al.
Applicant..... Microsoft Corporation
Attorney's Docket No. MS1-595US
Title: Integrating Payment Accounts And An Electronic Wallet

TRANSMITTAL LETTER AND CERTIFICATE OF MAILING

To: Commissioner of Patents and Trademarks
Washington, D.C. 20231
From: Allan T. Sponseller (509) 324-9256
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

The following enumerated items accompany this transmittal letter and are being submitted for the matter identified in the above caption.

1. Transmittal Letter with Certificate of Mailing included.
2. PTO Return Postcard Receipt
3. Check in the Amount of \$1528.00
4. Fee Transmittal
5. New patent application (title page plus 46 pages, including claims 1-47 & Abstract)
6. Executed Declaration
7. 8 sheets of formal drawings (Figs. 1-8)
8. Assignment w/Recordation Cover Sheet

Large Entity Status ☒ Small Entity Status ☐

The Commissioner is hereby authorized to charge payment of fees or credit overpayments to Deposit Account No. 12-0769 in connection with any patent application filing fees under 37 CFR 1.16, and any processing fees under 37 CFR 1.17.

Date: Sept 28, 2000

By: [Signature]
Allan T. Sponseller
Reg. No. 38,318

CERTIFICATE OF MAILING

I hereby certify that the items listed above as enclosed are being deposited with the U.S. Postal Service as either first class mail, or Express Mail if the blank for Express Mail No. is completed below, in an envelope addressed to The Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the below-indicated date. Any Express Mail No. has also been marked on the listed items.

Express Mail No. (if applicable) EL685271484

Date: 9/28/2000
By: [Signature]
Dana L. Calhoun

EL685271484

JCS25 U.S. PTO
09/675467

09/28/00

PTO/SB/17 (08-00)

Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**FEE TRANSMITTAL
for FY 2000**

Patent fees are subject to annual revision.

Complete if Known

Application Number	
Filing Date	9/28/2000
First Named Inventor	Blinn
Examiner Name	
Group Art Unit	
Attorney Docket No.	MSI-624US

TOTAL AMOUNT OF PAYMENT (\$1528⁰⁰)**METHOD OF PAYMENT (check one)**

- 1.
- ☒
- The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number 12-0769

Deposit Account Name Lee & Hayes PLLC

- ☒
- Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR 1.27

- 2.
- ☒
- Payment Enclosed:

☒ Check ☐ Credit card ☐ Money Order ☐ Other**FEE CALCULATION****1. BASIC FILING FEE**

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
101 690	201 345	Utility filing fee	690
106 310	206 155	Design filing fee	
107 480	207 240	Plant filing fee	
108 690	208 345	Reissue filing fee	
114 150	214 75	Provisional filing fee	

SUBTOTAL (1) (\$690⁰⁰)**2. EXTRA CLAIM FEES**

Total Claims	Extra Claims	Fee from below	Fee Paid
47	-20** = 27	18	486
7	-3** = 4	78	312
Multiple Dependent			

**or number previously paid, if greater; For Reissues, see below

Large Entity Small Entity

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description
103 18	203 9	Claims in excess of 20
102 78	202 39	Independent claims in excess of 3
104 260	204 130	Multiple dependent claim, if not paid
109 78	209 39	** Reissue independent claims over original patent
110 18	210 9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) (\$798⁰⁰)**FEE CALCULATION (continued)****3. ADDITIONAL FEES**

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
105 130	205 65	Surcharge - late filing fee or oath	
127 50	227 25	Surcharge - late provisional filing fee or cover sheet	
139 130	139 130	Non-English specification	
147 2,520	147 2,520	For filing a request for ex parte reexamination	
112 920*	112 920*	Requesting publication of SIR prior to Examiner action	
113 1,840*	113 1,840*	Requesting publication of SIR after Examiner action	
115 110	215 55	Extension for reply within first month	
116 380	216 190	Extension for reply within second month	
117 870	217 435	Extension for reply within third month	
118 1,360	218 680	Extension for reply within fourth month	
128 1,850	228 925	Extension for reply within fifth month	
119 300	219 150	Notice of Appeal	
120 300	220 150	Filing a brief in support of an appeal	
121 260	221 130	Request for oral hearing	
138 1,510	138 1,510	Petition to institute a public use proceeding	
140 110	240 55	Petition to revive - unavoidable	
141 1,210	241 605	Petition to revive - unintentional	
142 1,210	242 605	Utility issue fee (or reissue)	
143 430	243 215	Design issue fee	
144 580	244 290	Plant issue fee	
122 130	122 130	Petitions to the Commissioner	
123 50	123 50	Petitions related to provisional applications	
126 240	126 240	Submission of Information Disclosure Stmt	
581 40	581 40	Recording each patent assignment per property (times number of properties)	40
146 690	246 345	Filing a submission after final rejection (37 CFR § 1.129(a))	
149 690	249 345	For each additional invention to be examined (37 CFR § 1.129(b))	
179 690	279 345	Request for Continued Examination (RCE)	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$40⁰⁰)**SUBMITTED BY**

Name (Print/Type)	Allan T. Sponseller	Registration No. (Attorney/Agent)	38,318	Telephone	(509) 324-9256
Signature	<i>MTS</i>	Date	Sept. 28, 2000		

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

1, 11, 17, 21, 26, 35, 43

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Method and System for Restricting the Usage of
Payment Accounts**

Inventor(s):

Arnold N. Blinn
Joseph N. Coco

ATTORNEY'S DOCKET NO. MS1-624US

1 **TECHNICAL FIELD**

2 This invention relates to electronic commerce, and more particularly to
3 restricting the usage of payment accounts.
4

5 **BACKGROUND OF THE INVENTION**

6 As computer systems throughout the world are becoming increasingly
7 connected via the Internet, the uses for the Internet are similarly expanding. One
8 rapidly growing use of the Internet is for electronic commerce, where merchants
9 make goods and/or services available for purchase "on-line" via the Internet. Such
10 purchases may be delivered via the Internet (e.g., software downloaded from the
11 merchant to the purchaser's computer) or alternatively delivered via more
12 traditional in-person routes (e.g., mailing a product using the postal service).

13 Although the types and sources of goods and/or services available for
14 purchase on-line have increased, difficulties have been encountered in providing a
15 way for users to pay for these purchases. One solution is to provide an electronic
16 wallet for each user where he or she can store account and address information for
17 multiple different types of accounts, such as credit cards, debit cards, gift
18 certificates, rebates, etc. One such solution is described in co-pending application
19 no. 09/_____, attorney docket no. MS1-595US, entitled "Integrating Payment
20 accounts And An Electronic Wallet", to Arnold Blinn, Joseph Coco, and Greg
21 Marks.

22 However, problems can be encountered when using electronic wallets
23 because there is typically little or no ability to restrict the usage of accounts
24 identified in the wallet. While a credit card stored in a wallet could be spent at any
25 location that accepts this credit card, it may be desirable for other types of

1 accounts to be restricted in how they can be spent. It would be desirable, for
2 example, for a gift certificate account to be redeemable only at a restricted set of
3 merchants. If the gift certificate account is a new payment account mechanism
4 this restriction can be built into the protocol for redemption of the gift certificate.
5 However, a gift certificate account may be based on a credit card network (e.g.
6 Visa®) and credit card account numbering format (e.g., based on a Visa® card
7 format). Although the giver of the gift certificate may wish that the recipient use
8 the gift certificate at only certain merchants, if the gift certificate is based on the
9 Visa® account number format there is typically nothing preventing the recipient
10 from using the gift certificate anywhere that a Visa® card is accepted.

11 The invention described below addresses these disadvantages, providing
12 restricted usage of payment accounts.

13 14 **SUMMARY OF THE INVENTION**

15 A method and system for restricting the usage of payment accounts is
16 described herein.

17 According to one aspect, payment accounts maintained in an electronic
18 wallet are restricted to being spent at only a particular set of one or more
19 merchants. The set of merchants can be a static set, or alternatively a dynamic set
20 with the merchants that belong to the set changing over time. When the user
21 attempts to purchase goods and/or services at a merchant using a particular
22 payment account, a check is made to verify that the restrictions on the payment
23 account permit the user to make purchases at that merchant.

24 According to another aspect, restrictions limit the ability of funds to be
25 transferred into payment accounts or transferred to other payment accounts. The

1 payment account is limited so that funds can be added to (or withdrawn from) the
2 payment account only from (or to) certain individuals. Such limitations prevent
3 the user from transferring funds to particular other individuals, or receiving funds
4 from particular other individuals (e.g., a parent may establish a child's payment
5 account so that only the parent can add funds to it, not other individuals the child
6 may encounter on the Internet).

7 According to another aspect, different payment accounts can be combined,
8 thereby increasing the funds in one of the accounts (or creating a new payment
9 account). When combining accounts, the restrictions on the newly created account
10 (or account with increased funds) are a subset of the restrictions of the original
11 accounts that were combined. In other words, the newly created account (or
12 account with increased funds) can only be used in the same manner as both of the
13 source accounts could have been used.

14 According to another aspect, merchant-specific payment accounts can be
15 established and corresponding physical cards (e.g., credit cards or smart cards)
16 issued to users. An account number is stored on the card along with restrictions
17 that limit the card to being used only at the specific merchant. The new payment
18 account information is also communicated to an account processing network so
19 that subsequent use of the card can be verified. This system allows merchants to
20 issue payment accounts (e.g., gift certificates or rebates) taking advantage of an
21 account processing network managed by someone other than the merchant.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings. The same numbers are used throughout the figures to reference like components and/or features.

Fig. 1 is a block diagram illustrating an exemplary network environment such as may be used in accordance with certain embodiments of the invention.

Fig. 2 illustrates an example of a suitable operating environment in which at least portions of the invention may be implemented.

Fig. 3 illustrates an exemplary suite of services including an electronic wallet such as may be used in certain embodiments of the invention.

Fig. 4 is a block diagram illustrating an exemplary environment in which purchases of goods and/or services can be made using an electronic wallet.

Fig. 5 is a block diagram illustrating an exemplary data flow when making a purchase from a merchant Web page using an electronic wallet in accordance with certain embodiments of the invention.

Fig. 6 is a flowchart illustrating an exemplary process for displaying accounts useable for a purchase in accordance with certain embodiments of the invention.

Fig. 7 is a flowchart illustrating an exemplary process for imposing restrictions on payment accounts in accordance with certain embodiments of the invention.

Fig. 8 is a block diagram illustrating an exemplary process for distribution and use of a merchant-specific payment account in accordance with certain embodiments of the invention.

DETAILED DESCRIPTION

Fig. 1 is a block diagram illustrating an exemplary network environment such as may be used in accordance with certain embodiments of the invention. In the network environment 100 of Fig. 1, multiple clients 102, multiple merchant servers 104, and a wallet server 106 are illustrated coupled together via a network 108. Network 108 represents any of a wide variety of wired and/or wireless networks, including public and/or private networks (such as the Internet, local area networks (LANs), wide area networks (WANs), etc.). Clients 102 and servers 104, 106 can be coupled to network 108 in any of a wide variety of conventional manners, such as wired or wireless modems, direct network connections, etc.

Clients 102 communicate with servers 104, 106 using one or more conventional protocols. In one implementation, network 108 is the Internet which supports the World Wide Web. The World Wide Web (also referred to as simply the "Web") is a collection of documents (referred to as "Web pages") that users can view or otherwise render and which typically include links to one or more other pages that the user can access. Information is communicated among clients 102 and servers 104 using, for example, the Hypertext Transfer Protocol (HTTP), although other protocols (either public or proprietary) could alternatively be used. Web pages are created in a markup language, such as the Hypertext Markup Language (HTML) or the eXtensible Markup Language (XML), although other languages could alternatively be used.

Wallet server 106 maintains an electronic "wallet" for each of multiple users of clients 102. Inside his or her electronic wallet, a user is able to store information regarding various accounts, some of which are traditional credit card

1 accounts and others of which are referred to as "payment accounts". As used
2 herein, a "payment account" refers to an account that has a monetary value
3 associated with it (which may be changed), rather than a line of credit as is
4 associated with traditional credit card accounts. The user is able, via a Web
5 browser 110 running on a client 102, to use the payment accounts to make
6 purchases on-line and also to manipulate the payment accounts. Such
7 manipulation includes, for example, setting up new payment accounts, changing
8 information in previously created payment accounts, adding funds to payment
9 accounts, transferring value between payment accounts, etc.

10 During operation, Web browser 110 accesses a Web page hosted by a
11 merchant server 104. A user is able, via Web browser 110, to purchase goods
12 and/or services from the merchant via the Web page hosted by the merchant server
13 104. During the purchasing process, Web browser 110 receives, from wallet
14 server 106, an indication of the accounts (including payment accounts and
15 traditional credit card accounts) available to the user. Web browser 110 allows the
16 user to select one of these available accounts to purchase the goods and/or
17 services, and forwards payment information for the selected account to the
18 merchant server 104.

19 Various restrictions can be imposed on the payment accounts during
20 operation on a per-account basis. Such restrictions limit the ability of the user to
21 spend funds from his or her account(s) and/or the ability of the user to receive
22 additional funds into his or her pre-existing account(s). By so restricting the
23 payment accounts, the accounts can be maintained in a centralized location for
24 easy identification and access by the user, while at the same time allowing the
25

1 user's ability to spend and/or receive funds from or to the different accounts to be
2 limited.

3 Fig. 2 illustrates an example of a suitable operating environment in which
4 at least portions of the invention may be implemented. The illustrated operating
5 environment is only one example of a suitable operating environment and is not
6 intended to suggest any limitation as to the scope of use or functionality of the
7 invention. Other well known computing systems, environments, and/or
8 configurations that may be suitable for use with the invention include, but are not
9 limited to, personal computers, server computers, hand-held or laptop devices,
10 multiprocessor systems, microprocessor-based systems, programmable consumer
11 electronics, gaming consoles, cellular telephones, public terminals or kiosks,
12 wearable computers, network PCs, minicomputers, mainframe computers,
13 distributed computing environments that include any of the above systems or
14 devices, and the like.

15 Alternatively, the invention may be implemented in hardware or a
16 combination of hardware, software, and/or firmware. For example, one or more
17 application specific integrated circuits (ASICs) could be designed or programmed
18 to carry out the invention.

19 Fig. 2 shows a general example of a computer 142 that can be used in
20 accordance with the invention. Computer 142 is shown as an example of a
21 computer that can perform the functions of a client 102 or server 104 or 106 of
22 Fig. 1. Computer 142 includes one or more processors or processing units 144, a
23 system memory 146, and a bus 148 that couples various system components
24 including the system memory 146 to processors 144.

1 The bus 148 represents one or more of any of several types of bus
2 structures, including a memory bus or memory controller, a peripheral bus, an
3 accelerated graphics port, and a processor or local bus using any of a variety of
4 bus architectures. The system memory 146 includes read only memory (ROM)
5 150 and random access memory (RAM) 152. A basic input/output system (BIOS)
6 154, containing the basic routines that help to transfer information between
7 elements within computer 142, such as during start-up, is stored in ROM 150.
8 Computer 142 further includes a hard disk drive 156 for reading from and writing
9 to a hard disk, not shown, connected to bus 148 via a hard disk drive interface 157
10 (e.g., a SCSI, ATA, or other type of interface); a magnetic disk drive 158 for
11 reading from and writing to a removable magnetic disk 160, connected to bus 148
12 via a magnetic disk drive interface 161; and an optical disk drive 162 for reading
13 from and/or writing to a removable optical disk 164 such as a CD ROM, DVD, or
14 other optical media, connected to bus 148 via an optical drive interface 165. The
15 drives and their associated computer-readable media provide nonvolatile storage
16 of computer readable instructions, data structures, program modules and other data
17 for computer 142. Although the exemplary environment described herein employs
18 a hard disk, a removable magnetic disk 160 and a removable optical disk 164, it
19 will be appreciated by those skilled in the art that other types of computer readable
20 media which can store data that is accessible by a computer, such as magnetic
21 cassettes, flash memory cards, random access memories (RAMs), read only
22 memories (ROM), and the like, may also be used in the exemplary operating
23 environment.

24 A number of program modules may be stored on the hard disk, magnetic
25 disk 160, optical disk 164, ROM 150, or RAM 152, including an operating system

1 170, one or more application programs 172, other program modules 174, and
2 program data 176. A user may enter commands and information into computer
3 142 through input devices such as keyboard 178 and pointing device 180. Other
4 input devices (not shown) may include a microphone, joystick, game pad, satellite
5 dish, scanner, or the like. These and other input devices are connected to the
6 processing unit 144 through an interface 168 that is coupled to the system bus
7 (e.g., a serial port interface, a parallel port interface, a universal serial bus (USB)
8 interface, etc.). A monitor 184 or other type of display device is also connected to
9 the system bus 148 via an interface, such as a video adapter 186. In addition to the
10 monitor, personal computers typically include other peripheral output devices (not
11 shown) such as speakers and printers.

12 Computer 142 operates in a networked environment using logical
13 connections to one or more remote computers, such as a remote computer 188.
14 The remote computer 188 may be another personal computer, a server, a router, a
15 network PC, a peer device or other common network node, and typically includes
16 many or all of the elements described above relative to computer 142, although
17 only a memory storage device 190 has been illustrated in Fig. 2. The logical
18 connections depicted in Fig. 2 include a local area network (LAN) 192 and a wide
19 area network (WAN) 194. Such networking environments are commonplace in
20 offices, enterprise-wide computer networks, intranets, and the Internet. In certain
21 embodiments of the invention, computer 142 executes an Internet Web browser
22 program (which may optionally be integrated into the operating system 170) such
23 as the "Internet Explorer" Web browser manufactured and distributed by
24 Microsoft Corporation of Redmond, Washington.

When used in a LAN networking environment, computer 142 is connected to the local network 192 through a network interface or adapter 196. When used in a WAN networking environment, computer 142 typically includes a modem 198 or other means for establishing communications over the wide area network 194, such as the Internet. The modem 198, which may be internal or external, is connected to the system bus 148 via a serial port interface 168. In a networked environment, program modules depicted relative to the personal computer 142, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

Computer 142 also includes a broadcast tuner 200. Broadcast tuner 200 receives broadcast signals either directly (e.g., analog or digital cable transmissions fed directly into tuner 200) or via a reception device (e.g., via antenna 110 or satellite dish 114 of Fig. 1).

Computer 142 typically includes at least some form of computer readable media. Computer readable media can be any available media that can be accessed by computer 142. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other media

1 which can be used to store the desired information and which can be accessed by
2 computer 142. Communication media typically embodies computer readable
3 instructions, data structures, program modules or other data in a modulated data
4 signal such as a carrier wave or other transport mechanism and includes any
5 information delivery media. The term "modulated data signal" means a signal that
6 has one or more of its characteristics set or changed in such a manner as to encode
7 information in the signal. By way of example, and not limitation, communication
8 media includes wired media such as wired network or direct-wired connection,
9 and wireless media such as acoustic, RF, infrared and other wireless media.
10 Combinations of any of the above should also be included within the scope of
11 computer readable media.

12 The invention has been described in part in the general context of
13 computer-executable instructions, such as program modules, executed by one or
14 more computers or other devices. Generally, program modules include routines,
15 programs, objects, components, data structures, etc. that perform particular tasks
16 or implement particular abstract data types. Typically the functionality of the
17 program modules may be combined or distributed as desired in various
18 embodiments.

19 For purposes of illustration, programs and other executable program
20 components such as the operating system are illustrated herein as discrete blocks,
21 although it is recognized that such programs and components reside at various
22 times in different storage components of the computer, and are executed by the
23 data processor(s) of the computer.

24 Fig. 3 illustrates an exemplary suite of services including an electronic
25 wallet such as may be used in certain embodiments of the invention. The suite of

1 services 220 includes an electronic wallet 222, an authentication module 224, and
2 optionally an account monitor 227. The suite of services 220 may be made
3 available to users from the same remote server (such as server 106 of Fig. 1) or
4 alternatively different servers (for example, electronic wallet 222 may be made
5 available from the first server while authentication module 224 is made available
6 from another server).

7 In the illustrated example, a user first signs in or logs in to services 220
8 using his or her Web browser. This sign-in may be accomplished directly by the
9 user accessing a Web page hosted by the server that provides services 220, or
10 alternatively indirectly by the user accessing another Web page that redirects the
11 user's Web browser to services 220. Sign-in is managed by authentication module
12 224, which verifies the identity of the user signing in. This verification can be
13 performed in any of a wide variety of conventional manners, such as using a user
14 ID and associated password, as well as any of numerous cryptographic and other
15 techniques for authenticating the user. Once the user's identity is verified, the user
16 is able to access the information maintained by services 220.

17 Electronic wallet 222 stores various purchasing and address information for
18 a user. This stored information includes user identification information 228,
19 address information 230, and information for multiple accounts (including both
20 payment accounts and traditional credit card accounts) 232. User identification
21 information 228 includes various information uniquely identifying the user
22 electronic wallet 222 belongs to as well as information about the user's electronic
23 wallet. Table I identifies the user identification information maintained in one
24 exemplary implementation.
25

Table I

Name	Description
MemberId	The user ID.
ProfileVersion	An incremental counter starting at 1 and incremented each time the electronic wallet is updated/modified.
CurrentAddress	The AddressID of one of the user's addresses. Often used as the default shipping address for purchased goods and/or services.
CurrentCard	The ID of one of the user's accounts, which can be a payment account or traditional credit card account.

Address information 230 includes various addresses corresponding to the user. These addresses can include, for example, a home address, a business address, shipping addresses for the user or others (e.g., friends or family), a credit card billing address, etc. Table II identifies the information maintained for each address in one exemplary implementation.

Table II

Name	Description
AddressID	Unique (for the user) identifier of the address.
MemberId	The user ID.
Fname	First name of person for address.
Lname	Last name of person for address.
Addr1	First line of address (e.g., to include company or street name).
Addr2	Second line of address (e.g., to include street name or apartment number).
City	City for address.
State	State for address.
PostalCode	Postal code for address.
Country	Country for address.
Phone	Phone number corresponding to address.
Email	Email corresponding to address (could be the user, the person identified in Fname and Lname fields, or someone else).
FriendlyName	User-friendly identifier of the address (e.g., "Home", "Mom's Address", etc.).

Multiple accounts 232 are illustrated with the electronic wallet 222. In the illustrated example, two credit cards 236, 238, a gift certificate 240, a rebate account 242, a debit card 244, a cash account 246, an allowance account 248, and a reward account 249 are shown. It is to be appreciated that these accounts illustrated are exemplary only, and alternatively more or fewer accounts could be included in electronic wallet 222. Additionally, other types of accounts (not shown), such as Micro Payment accounts, may also be included in electronic wallet 222. Credit card accounts are accounts that correspond to the user's physical credit cards. Gift certificate payment accounts are accounts that correspond to electronic gift certificates that have been given (or otherwise transferred) to the user. Rebate payment accounts are accounts that correspond to electronic rebates that have been given (or otherwise transferred) to the user, such

1 as in response to the user's purchase of a particular product. Reward payment
2 accounts are accounts that correspond to rewards that have been given to the user
3 in exchange for certain behavior (e.g., accessing certain web sites, making
4 donations, being a long-term customer, registering a product within a certain
5 period of time, etc.). Debit card payment accounts are accounts that correspond to
6 the user's physical debit cards (e.g., as issued by a bank). Cash payment accounts
7 are accounts that are analogous to physical cash carried by the user. Cash
8 payment accounts are similar to debit card payment accounts in that they have a
9 limited amount of funds associated with them and do not involve issuance of
10 credit to the user. Allowance payment accounts are a special type of cash or debit
11 card payment account that are designed to be given to children (with the advantage
12 of restricting the usage of the account)

13 Different types of accounts (e.g., credit cards, debit cards, gift certificates,
14 rebates, rewards, cash, allowance, etc.) can be included in electronic wallet 222, as
15 well as multiple accounts of the same type. Each of the different types of accounts
16 is presented differently to the user, allowing him or her to easily distinguish
17 between accounts. In some instances, logos corresponding to the account type
18 (e.g., Visa®) or the issuer (e.g., the bank name) may be displayed to the user.
19 However, even though the different account types are presented to the user
20 differently, the different account types may share an underlying format. For
21 example, gift certificates may use the same account numbering scheme as is used
22 for Visa® cards.

23 Each of the accounts 232 includes payment information for the account.
24 This payment information includes information that is passed to a merchant server
25 to allow the user to purchase goods and/or services from a merchant. Table III

identifies the information maintained for each account 232 in one exemplary implementation. Note, however, that not all accounts need include all of this information, and other accounts may include additional information.

Table III

Name	Description
ID	Unique (for the user) identifier of the account.
MemberId	The user ID.
Type	An identifier of the type of account.
Num	An account number for the account. For credit cards, the credit card number.
Num2	A secondary number for identifying the card. For Visa cards this could be the CVV2 (Card Verification Value 2).
Exp	An expiration date of the account.
BillingAddress	The AddressID of one of the address in the Addresses table.
Name	The name on the account.
FriendlyName	A user-friendly identifier of the account (e.g., "Joe's Visa", "Gift Certificate From Mom", "Rebate from Microsoft®").
Restrictions	Restrictions associated with the payment account (e.g., where funds corresponding to the payment account can be spent or where new funds to be added to the payment account can be received from).

Services 220 can be accessed by client Web browsers 250 for a variety of different purposes. A user may access services 220 directly, such as to modify information in electronic wallet 222 (e.g., add a new payment account, change an address, etc.). Modifications to electronic wallet 222 may also be made by others, as discussed in more detail below. A wallet manager 234 transmits web pages to browser 250 with options allowing a user to add, delete, and modify accounts 232 and addresses 230. A user may also access services 220 indirectly, such as when making a purchase of goods or services from a merchant Web page 252. During

1 the purchasing process, Web browser 250 acts as an intermediary between the
2 merchant Web page 252 and electronic wallet 222, as discussed in more detail
3 below.

4 When included in services 222, account monitor 227 monitors the usage of
5 payment accounts within accounts 232 and prevents transactions if the restrictions
6 on a payment account are violated. In one implementation, transactions involving
7 the transfer of funds to and/or from payment accounts are passed through account
8 monitor 227 prior to being returned to the requesting web browser 250. Account
9 monitor 227 compares the identity of the recipient of funds from a payment
10 account (or alternatively the source of funds for a payment account) to the
11 restrictions associated with the payment account. If the restrictions indicate that
12 the recipient (or source) is acceptable, then account monitor 227 allows the
13 transfer to continue. However, if the restrictions indicate that the recipient (or
14 source) is unacceptable, then account monitor 227 prohibits the transfer. Account
15 monitor 227 can prohibit the transfer in any of a variety of manners, such as
16 simply returning an indication to web browser 250 that the transaction cannot be
17 completed.

18 Different types of restrictions can be imposed by the account monitor on
19 payment accounts on a per-payment account basis, limiting the user's ability to
20 spend the funds from payment accounts (or receive additional funds into payment
21 accounts). Restrictions on payment accounts can be classified into two general
22 types: merchant usage restrictions and payment account transfer restrictions.
23 Merchant usage restrictions refer to restrictions on where the user is able to spend
24 the funds in the payment account. Payment account transfer restrictions refer to
25

1 restrictions, for a particular payment account, on what other payment accounts the
2 user can receive funds from and/or transfer funds to.

3 Merchant usage restrictions limit where (e.g., based on the identity of the
4 merchant(s)) the user is able to spend funds associated with the payment account.
5 The payment account can be restricted to being spent at only a set of one or more
6 merchants. Which merchants the payment account can be spent at is identified
7 when the payment account is established. For example, if a mother is giving her
8 son a gift certificate payment account, then the mother can identify, during the
9 process of purchasing the gift certificate, which on-line merchant(s) the gift
10 certificate funds can be spent at. The set of one or more merchants can be a static
11 set or a dynamic set that changes over time. By way of example, the payment
12 account may identify a static set of merchants (e.g., by name, numeric identifier,
13 by Internet address, etc.) that funds associated with the account can be spent at.
14 Alternatively, the payment account may identify a particular group of merchants
15 (e.g., those corresponding to a particular on-line community, such as an on-line
16 shopping mall). An example of such a group of merchants are the MSN®
17 Shopping merchants accessible via the MSN® Web site. The actual merchants
18 within the group may change over time, and the restriction imposed on the
19 payment account is checked when funds for the payment account are to be spent –
20 if the merchant where funds are to be spent is part of the group at the time the
21 funds are to be spent, then the purchase is allowed; otherwise, the purchase is not
22 allowed, even if the merchant were a part of the group when the payment account
23 was created.

24 Merchant usage restrictions can further limit the user's ability to use the
25 payment account off-line. For example, the restrictions may indicate whether a

physical card (e.g., analogous to a credit card or smart card) can be issued to the user. If such a physical card can be issued to the user, then the user is able to spend the funds from the payment account in a traditional off-line manner using the physical card. The restrictions may also indicate whether the user can obtain "cash" from the account, including cash in-hand, transfer to a checking or savings account, etc. (e.g., if a physical card is issued to the user, whether the physical card can be used at an automated teller machine (ATM) for the user to directly withdraw funds from the payment account).

Payment account transfer restrictions limit the ability of the user to transfer funds from (or receive funds in to) one of his or her payment accounts to (or from) the payment account of another. A payment account may be restricted to transferring funds to only one or more other users (e.g., identified by some unique identifier such as an email address). A payment account may similarly be restricted to receiving funds from only one or more other users. For example, an allowance payment account used by a child may be limited to receiving funds only from the child's parents.

The restrictions on payment accounts also limit the user's ability to combine funds from multiple ones of his or her payment accounts. By way of example, assume that a user has two \$50 gift certificates: one is restricted to being spent only at Merchants A, B, and C, while the other is restricted to being spent only at Merchants C, D, and E. If the user desires to make a \$100 purchase at Merchant C, then the user can combine both gift certificates for the purchase (because both certificates are useable at Merchant C). This would also entail either creating a new gift certificate account that is redeemable only at Merchant C, or alternatively modifying the restrictions on the account the two are combined

1 into to being redeemable only at Merchant C. However, if the user desires to
2 make a \$100 purchase at any one of Merchants A, B, D, or E, then the user is
3 limited to using only one of the \$50 gift certificates (having to come up with the
4 remaining \$50 from some other source).

5 Each payment account may also have an expiration date associated with it.
6 Once the expiration date has passed, the payment account is no longer valid and
7 cannot be used for purchases (the expiration date is compared to the current date at
8 the time the funds are trying to be spent, and authorization to spend the funds fails
9 if the expiration date has passed). If two payment accounts are combined, then the
10 resultant combination is also limited by the earliest expiration date of the two
11 accounts (if any). Following the previous example, assume that one of the \$50 gift
12 certificates has an expiration date of January 1, 1999 and the other has an
13 expiration date of June 1, 1999. The newly created \$100 gift certificate (whether a
14 new account or one of the original accounts with new funds added to it) would
15 then have an expiration date of January 1, 1999.

16 The combination of funds into a payment account occurs prior to purchase,
17 and may be just before the purchase (e.g., when the user checks out at an on-line
18 merchant) or alternatively a substantial period of time prior to the purchase (e.g.,
19 weeks or months). If funds from multiple source payment accounts are to be
20 combined, then either a new payment account is created or the funds available on
21 one of the source payment accounts is increased (and the funds on the other source
22 payment account decreased). Regardless of whether a new payment account is
23 created or a pre-existing payment account is modified, the payment account that
24 the funds are transferred to has restrictions that satisfy the restrictions of both
25 source payment accounts. By way of example, assume that a user has two \$50 gift

certificates that he desires to combine into a single gift certificate: the first gift certificate is restricted to being spent only at Merchants A, B, and C, while the second gift certificate is restricted to being spent only at Merchants C, D, and E. If funds from the second gift certificate (either all or a portion of the funds) are to be transferred to the first gift certificate, then the restrictions on the first gift certificate are changed so that the first gift certificate is restricted to being spent only at Merchant C (or a new gift certificate is created that is restricted to being spent only at Merchant C).

The combination of payment accounts and creation of new restrictions may be a reversible or irreversible process. For instance, once funds from the second gift certificate in the previous example are added to the first gift certificate, the restriction changes on the first gift certificate may be irreversible (the funds from the first gift certificate will always be limited to being spent at Merchant C – no purchases from Merchants A or B can be made with the funds). Alternatively, the device performing the combining (e.g., wallet manager 234) may maintain a record of what combinations were made and allow them to be later reversed or “un-done” by the user. Additional limitations may be made on such reversals, such as allowing the reversal only if no funds from the combined account have been spent since the combination.

In addition to combining payment accounts, a single payment account may also be separated or "split" into multiple payment accounts. For example, a \$100 gift certificate may be separated into one \$50 gift certificate and two \$25 gift certificates. Each of the newly created payment accounts is restricted to being spent at the same merchants as the original payment account, and the expiration date of each of the newly created payment accounts is the same as the original

1 payment account. Analogous to the combining of payment accounts, the splitting
2 of payment accounts may be a reversible or irreversible process.

3 Electronic wallet 222 further provides a centralized location at which a user
4 can store all of the information necessary to make purchases on-line. The user can
5 have multiple different types of payment accounts in his or her wallet and have
6 them readily accessible regardless of their source. For example, the user need not
7 remember what gift certificates and/or rebates he or she has received, but simply
8 access his or her electronic wallet to identify the available gift certificates and
9 rebates. Additionally, using the centralized storage of accounts 232 and addresses
10 230, a user is able to simply select from already-entered data to make purchases at
11 a wide variety of on-line merchants, thereby reducing the amount of data entry
12 required by the user and reducing the chances of errors in entering the information
13 at numerous locations.

14 Fig. 4 is a block diagram illustrating an exemplary environment in which
15 purchases of goods and/or services can be made using an electronic wallet. The
16 user of a client 102, via a Web browser 110 running on client 102, can access both
17 a merchant server 104 and wallet server 106. Wallet server 106 includes multiple
18 electronic wallets 272, 274, and 276, each corresponding to a different user. The
19 user can manipulate funds in his or her wallet, and has no access to wallets of
20 other users stored on wallet server 106.

21 A user can receive funds into, or spend funds from, any of the accounts
22 identified in his or her electronic wallet (subject to any restrictions on the payment
23 accounts). The receipt or expenditure of funds can be performed directly from
24 wallet server 106 (e.g., a user transferring funds from one of his or her payment
25 account accounts to the account of another user), or indirectly from wallet server

1 106 (e.g., via a merchant server 104). It should be noted, however, that the
2 payment accounts within an electronic wallet only identify accounts and money
3 that the user has access to – the payment accounts do not actually store money
4 themselves. For example, a debit card payment account may store a debit card
5 number and corresponding expiration date. However, the actual money for the
6 account (the funds that the user has access to using that debit card) is maintained
7 by the bank (or other issuer) of the debit card.

8 When funds are being transferred from a payment account to a merchant
9 (e.g., being spent), the identification information stored in the electronic wallet for
10 the payment account (e.g., account number, fraud protection number (if any),
11 expiration date (if any), and billing address (if any)) is transferred first to the
12 merchant and then from the merchant to the issuing bank (or agent thereof) 278.
13 This first transfer (to the merchant) can be simply done through an HTTP POST
14 from the wallet server to the merchant server. This second transfer (to the issuing
15 bank) is typically performed by communicating the information to a universal
16 credit card platform or network 280, such as that provided by First Data Corp.
17 (FDC) of Atlanta, GA. The universal credit card platform 280 verifies the
18 integrity of the account number and the funds available, and reports the
19 information to the requester (e.g., merchant server 104). Account number
20 integrity can be verified in any of a wide variety of conventional manners.
21 Alternatively, rather than communicating directly with the platform 280, the
22 requester may communicate with platform 280 via an intermediary 282.
23 Intermediary 282 may, for example, receive information for multiple purchases
24 and combine them for submission to platform 280 as a group.
25

Note that certain account types (e.g., gift certificates payment accounts) might not be backed by a traditional bank or credit card. A simple account and account balance might be maintained in such situations (e.g., at wallet server 106 or another device), although the principles of spending it are the same as above.

Funds can be transferred into a payment account from other accounts in the same electronic wallet (e.g., combining accounts), or alternatively from external sources. To receive funds into a payment account, wallet manager 234 receives an indication of the payment account the funds are to be transferred into and verifies the availability of the funds (e.g., via intermediary 282 or universal credit card platform 280), analogous to the merchant's verification of fund availability discussed above. Assuming the desired funds are available (and the addition of funds to the payment account is not restricted), the wallet server adds the funds to the indicated payment account by forwarding an indication of the desired funds to the appropriate payment account issuer (e.g., via intermediary 282 or universal credit card platform 280), or by updating the appropriate indication in the electronic wallet (e.g., if the electronic wallet holds the funds). Similarly, the wallet server removes the funds from the source account by forwarding an indication of the removal (or other charge) to the appropriate source account issuer (e.g., via intermediary 282 or universal credit card platform 280).

Additionally, payment accounts can be added to an electronic wallet 222 by the user that corresponds to the wallet 222 or alternatively another user. For example, a user may desire to enter information for a new payment account, such as a new debit card he or she recently received. The user signs-in to his or her electronic wallet 222 via authentication module 224 and adds the information for

1 the new payment account via an interface (e.g., web pages) presented by wallet
2 manager 234.

3 Additionally, users may add payment accounts to other users' electronic
4 wallets either directly or indirectly. To directly add a payment account to another
5 user's electronic wallet (e.g., a new allowance account or an increase in the amount
6 of funds in an allowance account), the user signs in to his or her own electronic
7 wallet, and then identifies, via wallet manager 234, the other user that the new
8 payment account is to be added to. Such additions may be automatic, or
9 alternatively the other user may be prompted (e.g., the next time he or she signs-in
10 to his or her account) to approve the receipt. To indirectly add a payment account
11 to another user's account (e.g., a gift certificate or rebate), the user operates
12 through an intermediary (such as an electronic mail system). The intermediary
13 forwards an indication (e.g., an email message) to the user of the new payment
14 account. The user can either copy information from the email message himself or
15 herself to create the new payment account, or alternatively select a link embedded
16 in the email message. Selection of the email message causes the source of the new
17 payment account (e.g., a gift certificate or rebate portal) to communicate with the
18 wallet manager 234, identifying the user that the new payment account is to be
19 added for.

20 An account monitor 284 can be implemented in any one or more of wallet
21 server 106, intermediary 282, universal credit card platform 280, and or a bank
22 278. Account monitor 284 monitors the fund transfers for accounts maintained in
23 electronic wallets 272, 274, and 276, and verifies that the restrictions (if any)
24 imposed on such accounts are not being violated. If the restrictions are not being
25 violated, then the fund transfer is permitted and allowed to proceed; however, if

1 restrictions are being violated, then the fund transfer is denied and not allowed to
2 proceed. For example, if user B is attempting to spend funds from a gift certificate
3 payment account at Merchant A but the gift certificate payment account is
4 restricted to being spent only at Merchant D or Merchant E, then when the
5 attempted purchase is made account monitor 284 denies the purchase. When
6 account monitor 284 is implemented in intermediary 282, platform 280, or bank
7 278, the denial of a fund transfer can be indicated back to merchant server 104 (or
8 wallet server 106) with specific information as to why the transfer was denied
9 (e.g., an indication that restrictions were violated), or alternatively without such
10 specific information (e.g., simply indicating that the account cannot be verified for
11 the desired fund transfer).

12 Fig. 5 is a block diagram illustrating an exemplary data flow when making
13 a purchase from a merchant Web page using an electronic wallet in accordance
14 with certain embodiments of the invention. A user browses or "surfs" the Internet
15 via a browser 110 executing on a client 102. The user accesses one or more Web
16 pages 252 at a merchant server(s) that identify goods and/or services that the user
17 desires to purchase. The user selects these goods and/or services (act 300) in a
18 conventional manner via browser 110. When the goods and/or services are
19 selected, merchant server 104 displays a product purchase Web page 252 that
20 includes a link to electronic wallet 222 (act 302). The product purchase Web page
21 252 typically displays the products and/or services to the user and gives him or her
22 the option to purchase the displayed products and/or services by selecting the link
23 to electronic wallet 222. Often times, these product purchase Web pages are
24 referred to as "checkout" or "shopping cart" pages.
25

The user then selects (e.g., "clicks on") the link to the electronic wallet 222, which causes browser 110 to access wallet server 106 (act 304). Various information can be embedded in the link to the electronic wallet (e.g., included as parameters of a URL corresponding to wallet server 106). The amount of the user's desired purchase may also be embedded in the link. Table IV identifies the information embedded in the link to the electronic wallet in one exemplary implementation.

Table IV

Argument	Description
Partner ID	An identifier of the merchant site.
Language Code ID	Specifies the language to display the wallet pages in.
Return URL	URL that the wallet server should return to after user selections are made.
Data Requested	Identifies what data is requested by merchant server: e.g., shipping address only, account information only (including billing address, if any), or both shipping address and account information (with billing address). Allows only appropriate options to be presented to the user on the wallet page (e.g., account information is not displayed for user selection if the merchant only requests the shipping address).
Cards	List of accounts that are acceptable to the merchant.
Preferred Card	Identifies a preferred type of account, allowing the wallet page to include a logo or other identifier of the preferred type of account (either a traditional credit card account or a payment account).

The response by wallet server 106 varies, depending on whether the user of client 102 is already logged in to his or her wallet. If the user has not logged in to his or her wallet yet, then wallet server 106 connects browser 110 to a sign-in/authentication module (module 224 of Fig. 3). Authentication module 224

1 authenticates the user (act 306), associating the user of browser 110 with the
2 correct electronic wallet 222. This allows the correct one of multiple electronic
3 wallets stored at server 106 (that is, the electronic wallet that includes the user's
4 information) to be associated with the user of browser 110. Once the user is
5 logged in, a wallet page that includes the contents (or references to the contents) of
6 the user's electronic wallet 222 can be displayed to him or her (act 308). If, on the
7 other hand, the user is already logged in to his or her wallet, then the wallet page
8 can be displayed to the user (act 308) without making the user repeat the sign-in
9 process.

10 The wallet page displays to the user various information from his or her
11 electronic wallet 222. This information includes, for example, different accounts
12 232 from which the user can select to make his or her purchases, different
13 shipping addresses where the purchased goods are to be delivered (or purchased
14 services to be performed), different billing addresses that correspond to different
15 accounts 232, etc. These different options can be displayed to the user in a wide
16 variety of different manners, such as the use of drop-down or pull-down menus,
17 selection boxes with multiple entries (and optionally scroll bars), a radio button
18 corresponding to each selectable option, etc. In one implementation the billing
19 address is tied to the account, so selection of a new account automatically results
20 in selection of the appropriate billing address. The available options are controlled
21 by the merchant calling the wallet. For example, payment accounts not valid at
22 the merchant might not be displayed, or alternatively displayed but disabled.
23 Additionally, the specification of shipping address may be optional, as some
24 merchants do not require this (they do not need it or do not allow it to be different
25 than a billing address on a credit card).

1 Whatever options are selected by the user, their selection is forwarded to
2 wallet server 106 (act 310). Based on these selections, wallet server 106 accesses
3 electronic wallet 222 to obtain the purchase information for the selected account
4 and address information for the purchase (e.g., shipping address and billing
5 address for the account). This purchase information can include, for example, all
6 necessary information to use the identified account (e.g., in the case of an account
7 that is a credit card, the necessary information may include a billing address and
8 credit card number). Some of this information (e.g., a credit card number) may
9 not have been initially transferred to browser 110 (e.g., an indication of "My Visa"
10 may have been sent in act 308, but not the actual credit card number).

11 Wallet server 106 transfers this purchase information and address
12 information to browser 110 (act 312). This transfer is accomplished via an HTML
13 GET command, with at least some of the purchase and address information (e.g.,
14 the account number and expiration date) in hidden form fields. Upon receipt,
15 browser 110 issues an HTTPS (HTTP over SSL) POST to the merchant web page
16 (as indicated by the ReturnURL parameter in table IV), which forwards the
17 purchase and address information to merchant server 104 (act 314). Merchant
18 server 104 then has the necessary information to charge the purchase to the
19 appropriate account, allowing the merchant to be paid and the user to receive the
20 purchased goods and/or services. In one exemplary implementation, the purchase
21 and address information is transferred from browser 110 to merchant server 104 in
22 accordance with the well-known Electronic Commerce Modeling Language
23 (ECML).

24 Given the purchase and address information, merchant server 104 verifies
25 that the desired purchase can be made. Merchant server 104 validates the funds

1 through a bank (e.g., bank 278 of Fig. 4) or a protocol specific to the account type
2 being used to make the purchase. For example, for a Visa® account FDC could be
3 used, while for other accounts the protocol may be a proprietary protocol. By way
4 of another example, for a gift certificate payment account that conforms to the
5 Visa® card format (or is convertible to the Visa® card format), the payment
6 account would be validated through FDC, which communicates with a particular
7 bank on the back end that validates the funds for the payment account and
8 enforces any restrictions on the payment account.

9 Various security measures can optionally be implemented within the
10 process illustrated in Fig. 5 to maintain the security of confidential user
11 information. Examples of such security measures include establishing secure links
12 between client 102 and server 104 and/or server 106 (e.g., using the HTTPS
13 protocol), and encrypting information being passed.

14 In the illustrated example, wallet server 106 does not store an indication of
15 funds in the various payment accounts of a user's electronic wallet. Rather, if
16 such information is needed (e.g., to display to the user the funds still available to
17 him or her from a gift certificate) then wallet server 106 communicates with the
18 issuer of the account (e.g., via universal credit card platform 280) to obtain a
19 current balance available in the account. Alternatively, indications of funds
20 available in one or more payment accounts may be stored in the user's electronic
21 wallet. For example, the value of a rebate payment account may be stored in the
22 electronic wallet, and updated when the user spends a portion (or all) of the funds.

23 In situations where an identification of funds are stored in the user's
24 electronic wallet, then any transfers between accounts are accomplished by
25 updating the appropriate payment account balances in the electronic wallet.

1 However, in situations where an external entity needs to be made aware of the
2 transfer (e.g., the account issuer), then the account issuer is contacted to verify the
3 availability of funds to be transferred (e.g., via intermediary 282 or platform 280
4 of Fig. 4). If sufficient funds are available, then the appropriate charge is
5 communicated to the issuer of the source account and the appropriate addition is
6 communicated to the issuer of the destination account.

7 Wallet server 106 may also map one type of account to another type of
8 account. This mapping allows payment accounts to maintain their original identity
9 in the eyes of the user while at the same time allowing them to be viewed
10 differently by a merchant. By way of example, a gift certificate may be given to a
11 user. The gift certificate includes purchasing information in the Visa® credit card
12 format (or alternatively in a format that can be converted to the Visa® credit card
13 format). When the user accesses his or her wallet, he or she sees the gift
14 certificate as a gift certificate payment account – any association that the payment
15 account has with a Visa® card (or the Visa® card format) is hidden from the user.
16 However, when a purchase is made, wallet server 106 communicates the purchase
17 information for the gift certificate payment account to the merchant server as if the
18 purchase information were from a Visa® card. Any representation of the payment
19 account to the user as a gift certificate is thus hidden from the merchant. This has
20 the advantage of allowing the merchant to accept the payment without doing any
21 special work to accept a new payment account for purchase.

22 A user is able to maintain multiple different accounts in his or her
23 electronic wallet, and these accounts can be of the same or different types. Not all
24 merchants, however, may accept all of these different types of accounts. By way
25 of example, a user may store in his or her wallet two credit card accounts (one for

1 a Visa® card and one for an American Express® card) as well as a gift certificate
2 payment account. Although illustrated to the user as a gift certificate, the gift
3 certificate payment account may be of a format that can be converted to a Visa®
4 card format. A particular merchant (at which the gift certificate is redeemable), on
5 the other hand, may only accept the Visa® credit card for purchases. In this
6 example, the wallet server would thus include on the wallet page the Visa® card
7 account and the gift certificate payment account. The American Express® card
8 account would not be displayed because it is not useable by the user at that
9 merchant (and cannot be converted to a useable format). Alternatively, the non-
10 useable account(s) may be displayed to the user but displayed in a manner that
11 indicates that it is not useable (for example, it may be presented in a different font
12 or different color, or in a separate section identified as "not useable").

13 In the discussion above, various actions are described as being performed at
14 the wallet server. For example, conversions between account formats are
15 performed at the wallet server, purchase information for the accounts selected by
16 the user is retrieved in response to user selections, etc. Alternatively, some or all
17 of these actions may be carried out at the client (e.g., an applet executing in
18 browser 110 or other application executing on the client).

19 Fig. 6 is a flowchart illustrating an exemplary process for displaying
20 accounts useable for a purchase in accordance with certain embodiments of the
21 invention. The process of Fig. 6 is implemented by browser 110 and wallet server
22 106, and may be implemented in software.

23 Initially, a request for a user purchase is received from a merchant server
24 (act 350). The accounts that are useable at that merchant are then identified (act
25 352). These accounts can be identified in any of a wide variety of manners (e.g.,

1 the merchant may pre-register with the wallet server with the accounts, the request
2 received in act 350 may include them, etc.). The wallet server then selects a set of
3 accounts corresponding to the user that are useable at the merchant server (act
4 354). This set includes those accounts of a type that the merchant identified as
5 being useable, as well as those that are of a type that can be converted to a format
6 that is compatible with any one or more of those identified as being useable by the
7 merchant.

8 The set of accounts corresponding to the user that are useable at the
9 merchant server may optionally be further limited in act 352 based on the
10 restrictions on the payment accounts corresponding to the user. To limit the set of
11 accounts based on such restrictions, the wallet server communicates with an
12 account monitor (either implemented at the wallet server or elsewhere) to
13 determine whether the desired purchase would violate any of the restrictions
14 associated with the payment accounts corresponding to the user. If the purchase
15 would violate the restrictions of a particular one or more payment accounts, then
16 those payment accounts are not included in the selected set of accounts that are
17 useable at the merchant server.

18 The set of selected accounts is then presented (e.g., displayed) to the user
19 (act 356). The wallet server then receives a user selection of one of the accounts
20 in the set (act 358) and forwards the account purchasing information for that
21 account to the merchant server (act 360). This forwarding may be direct, or
22 alternatively via a Web browser.

23 Fig. 7 is a flowchart illustrating an exemplary process for imposing
24 restrictions on payment accounts in accordance with certain embodiments of the
25

1 invention. The process of Fig. 7 is implemented by an account monitor 284 of
2 Fig. 4, and may be implemented in software.

3 Initially, a fund transfer selection is received (act 380). The fund transfer
4 selection can be in response to a request to purchase goods and/or services from a
5 merchant, combine funds from multiple payment accounts, receive funds into
6 payment account, etc. Upon receipt of the selection, the account monitor
7 identifies any restrictions on the payment account (act 382) and determines
8 whether the transfer would violate any of those restrictions (act 384). If the
9 transfer would violate any of those restrictions then the transfer is denied (act
10 386); otherwise, the transfer is permitted (act 388).

11 Fig. 8 is a block diagram illustrating an exemplary process for distribution
12 and use of a merchant-specific payment account in accordance with certain
13 embodiments of the invention. A user 400 purchases a payment account from a
14 merchant 402. This purchase can be an in-person purchase (e.g., physically in the
15 merchant's store) or alternatively an on-line purchase (or purchase through some
16 other intermediary). Upon purchasing the payment account, merchant 402
17 delivers to user 400 a physical card 404 that corresponds to the payment account.
18 Physical card 404 can be created in any of a wide variety of manners, such as
19 including information identifying the payment account on a magnetic stripe on
20 card 404, in a memory device of card 404 (e.g., in the situation of a smart card),
21 etc. The information included on physical card 404 is the same information that
22 would be stored in the user's electronic wallet for a payment account (e.g., account
23 number, expiration date, fraud protection numbers, amount of funds in the
24 account, etc.) as well as restriction information that restricts usage of the payment
25 account to merchant 402.

1 Additionally, merchant 402 delivers to account processing network 406
2 (e.g., platform 280 of Fig. 4), account information 408. Account information 408
3 includes information necessary for network 406 to verify the authenticity of the
4 account for a subsequent purchase. Account information 408 also optionally
5 includes restriction information that restricts usage of the payment account to
6 merchant 402. Alternatively, merchant 402 may communicate account
7 information 408 to network 406 via an intermediary, such as wallet server 410.

8 Merchant 402 may also deliver to wallet server 410 (e.g., wallet server 106
9 of Fig. 4) account information 412 for the new payment account. Account
10 information 412 includes identifying information for the account (e.g., account
11 number, expiration date, fraud protection numbers, amount of funds in the
12 account, etc.) as well as restriction information that restricts usage of the payment
13 account to merchant 402. The account information 412 is stored in the electronic
14 wallet corresponding to user 400 at wallet server 410. Alternatively, the account
15 information 412 may be stored in the electronic wallet of another user that is
16 identified by user 400 (e.g., the intended recipient of the payment account, such as
17 for a gift certificate payment account).

18 When user 400 (or another individual using the payment account, such as
19 someone who received the payment account as a gift from user 400) attempts to
20 make a purchase in-person at merchant 402 using the physical card 404, the
21 account information (stored on card 404) is transmitted to account processing
22 network 406. Account processing network 406 verifies the integrity of the
23 account as well as the restrictions (which might be handled by the issuing
24 institution behind the bank ATM network, for example) and available funds, and
25 indicates the purchase can be permitted if the integrity and restrictions of the

1 account are satisfied and sufficient funds are available. Alternatively, user 400
2 may attempt to make an on-line purchase at merchant 402 using the account
3 information stored in his or her electronic wallet. The purchasing process in this
4 situation is the same, except that the account information is transmitted to account
5 processing network 406 from the user's electronic wallet on wallet server 410
6 rather than from physical card 404.

7 The payment account distribution and use system illustrated in Fig. 8
8 provides a mechanism via which merchants can easily distribute payment
9 accounts. These payment accounts can be issued in physical card format and/or
10 electronic format for storage in an electronic wallet. The system of Fig. 8 allows
11 merchants to take advantage of an account processing network 406, implemented
12 by someone other than the merchant, to manage payment accounts such as gift
13 certificates and rebates, thereby easing the management functions required of the
14 merchants to support such payment accounts.

15 There are many uses for this payment account distribution and use system
16 illustrated in Fig. 8. By way of example, a traditional "brick and mortar" merchant
17 is able to issue gift certificates in the form of plastic cards and/or an electronic
18 format that make use of an existing account processing network (e.g., in a Visa®
19 card format being verified via FDC) but that are redeemable only at that merchant.
20 Purchasing of these gift certificates can be via one or more merchant-branded web
21 pages, so that the account is displayed to the purchaser as being associated with
22 the merchant (and any use of the Visa® card format being hidden from the user).
23 This is particularly valuable for smaller merchants, as it relieves them of the
24 burden of establishing the account processing network themselves while at the
25 same time ensuring that the gift certificates it issues are redeemable only at that

1 merchant. By way of another example, an online merchant can sell gift
2 certificates in an analogous manner, issuing them in an electronic format and/or
3 plastic card format. Such gift certificates are thus also restricted to being
4 redeemed only at that merchant, yet the merchant is not required to establish the
5 account processing network to verify the gift certificates.

6 Although the description above uses language that is specific to structural
7 features and/or methodological acts, it is to be understood that the invention
8 defined in the appended claims is not limited to the specific features or acts
9 described. Rather, the specific features and acts are disclosed as exemplary forms
10 of implementing the invention.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CLAIMS

1. One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

receiving a request to make a purchase at an on-line merchant using funds from a payment account that is identified in an electronic wallet corresponding to a particular user;

identifying restrictions associated with the payment account;

comparing the restrictions to an identity of the on-line merchant; and

determining, based on the comparing, whether to allow the purchase to proceed.

2. One or more computer readable media as recited in claim 1, wherein the payment account comprises a debit card account.

3. One or more computer readable media as recited in claim 1, wherein the payment account comprises a gift certificate account.

4. One or more computer readable media as recited in claim 1, wherein the payment account comprises a rebate account.

5. One or more computer readable media as recited in claim 1, wherein the payment account comprises a cash account.

1 6. One or more computer readable media as recited in claim 1, wherein
2 the payment account comprises a reward account.

3
4 7. One or more computer readable media as recited in claim 1, wherein
5 the payment account comprises an allowance account.

6
7 8. One or more computer readable media as recited in claim 1, wherein
8 the restrictions limit the payment account to being used at one or more on-line
9 merchants that are part of a group of merchants that changes over time.

10
11 9. One or more computer readable media as recited in claim 1, wherein
12 the restrictions limit the payment account to being used at one or more on-line
13 merchants that are part of a static group of merchants.

14
15 10. One or more computer readable media as recited in claim 1, wherein
16 the plurality of instructions, when executed by the one or more processors, further
17 causes the one or more processors to perform acts including:

18 identifying an expiration date associated with the payment account;

19 comparing the expiration date to a current date; and

20 determining, based on the comparing of the expiration date to the current
21 date, whether to allow the purchase to proceed.

22
23 11. A system comprising:

24 an electronic wallet including a plurality of payment accounts; and
25

an account monitor, communicatively coupled to the electronic wallet, to restrict the transfer of funds from at least one of the plurality of payment accounts.

12. A system as recited in claim 11, wherein the account monitor restricts the transfer of funds to only a group of merchants that changes over time.

13. A system as recited in claim 11, wherein the account monitor restricts the transfer of funds to only a static group of merchants.

14. A system as recited in claim 11, wherein the account monitor further restricts the payment account to being combinable with only a particular one or more other payment accounts.

15. A system as recited in claim 11, wherein different ones of the plurality of payment accounts are restricted in different manners.

16. A system as recited in claim 11, wherein each of the plurality of payment accounts includes associated restrictions that are enforced by the account monitor.

17. A system comprising:
a wallet server including an electronic wallet having a plurality of payment accounts; and
a computing device, coupled to the wallet server, to restrict how funds can be transferred from at least one of the plurality of payment accounts.

1
2 **18.** A system as recited in claim 17, wherein the computing device
3 comprises an intermediary device coupled to both the wallet server and a universal
4 credit card platform.

5
6 **19.** A system as recited in claim 17, wherein the computing device
7 comprises at least a portion of a universal credit card platform.

8
9 **20.** A system as recited in claim 17, wherein the computing device is to
10 restrict how funds can be transferred in response to a user request to transfer
11 funds.

12
13 **21.** A system comprising:
14 an account interface to communicate, with an electronic wallet, regarding
15 payment accounts; and
16 an account monitor to restrict the ability to transfer funds of a payment
17 account corresponding to a particular user.

18
19 **22.** A system as recited in claim 21, wherein the account interface
20 comprises a web page.

21
22 **23.** A system as recited in claim 21, wherein the account interface
23 comprises an application.

1 **24.** A system as recited in claim 21, wherein the restricting comprises
2 limiting which of the plurality of on-line merchants the funds can be spent at.

3
4 **25.** A system as recited in claim 21, wherein the restricting comprises
5 limiting where funds to be added to the payment account can be received from.

6
7 **26.** A method comprising:
8 restricting where funds in a payment account, maintained in an electronic
9 wallet corresponding to a particular user, can be spent.

10
11 **27.** A method as recited in claim 26, wherein the restricting comprises
12 restricting whether funds can be transferred to another payment account.

13
14 **28.** A method as recited in claim 26, wherein the restricting comprises
15 restricting which on-line merchants the funds can be spent at.

16
17 **29.** A method as recited in claim 26, further comprising limiting, via an
18 expiration date, when the payment account can be spent.

19
20 **30.** A method as recited in claim 28, wherein the on-line merchants that
21 the funds can be spent at are a group of merchants that changes over time.

1 **31.** A method as recited in claim 26, further comprising restricting how
2 the funds in the payment account can be combined with funds from another
3 payment account prior to being spent.
4

5 **32.** A method as recited in claim 26, wherein the payment account
6 comprises one of: a credit card account, a debit card account, a gift certificate
7 account, a rebate account, a cash account, an allowance account, or a reward
8 account.
9

10 **33.** A method as recited in claim 26, further comprising restricting
11 different payment accounts in the electronic wallet in different manners.
12

13 **34.** One or more computer-readable memories containing a computer
14 program that is executable by a processor to perform the method recited in claim
15 26.
16

17 **35.** A method comprising:
18 restricting where funds to be added to a payment account in an electronic
19 wallet corresponding to a particular user can be received from.
20

21 **36.** A method as recited in claim 35, wherein the restricting comprises
22 allowing only a particular set of one or more additional users to add funds to the
23 payment account.
24
25

1 **37.** A method as recited in claim 35, wherein the electronic wallet is
2 maintained at a remote server.

3
4 **38.** A method as recited in claim 35, wherein the payment account
5 comprises a gift certificate account.

6
7 **39.** A method as recited in claim 35, wherein the payment account
8 comprises a cash account.

9
10 **40.** A method as recited in claim 35, further comprising restricting the
11 payment account to being combinable with only a particular one or more other
12 payment accounts.

13
14 **41.** A method as recited in claim 35, further comprising restricting
15 different payment accounts in the electronic wallet in different manners.

16
17 **42.** One or more computer-readable memories containing a computer
18 program that is executable by a processor to perform the method recited in claim
19 35.

20
21 **43.** A method comprising:
22 creating, by a merchant, a payment account corresponding to a particular
23 user;
24 verifying the authenticity of the payment account via a universal credit card
25 platform; and

1 allowing the funds in the payment account to be spent only at the merchant.

2
3 **44.** A method as recited in claim 43, further comprising issuing a
4 physical card corresponding to the payment account.

5
6 **45.** A method as recited in claim 43, further comprising adding the
7 payment account to an electronic wallet corresponding to the particular user.

8
9 **46.** A method as recited in claim 43, wherein the allowing comprises
10 associating restrictions with the payment account so that funds of the payment
11 account will only be approved for purchases made from the merchant.

12
13 **47.** One or more computer-readable memories containing a computer
14 program that is executable by a processor to perform the method recited in claim
15 43.

1 **ABSTRACT**

2 A user's ability to spend and/or receive funds for payment accounts
3 maintained in an electronic wallet are limited. These limitations include
4 restrictions on where the user is able to spend the funds in a payment account (e.g.,
5 at which merchants the funds can be spent, whether the funds can be withdrawn
6 from an ATM, etc.). These limitations may also include restrictions on what other
7 payment accounts the user can receive funds from and/or transfer funds to, thereby
8 limiting person-to-person fund transfers.
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

2023032912363

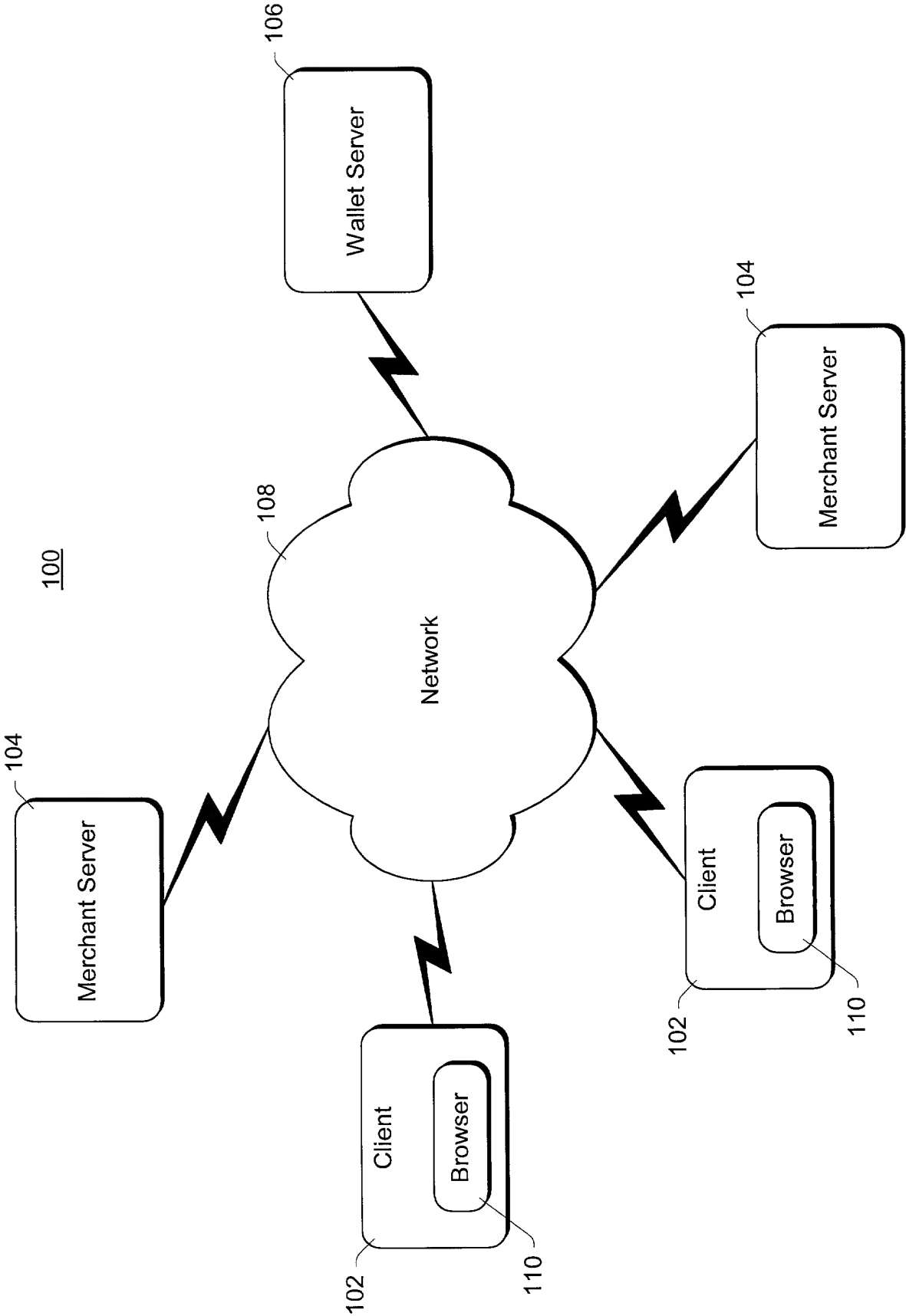
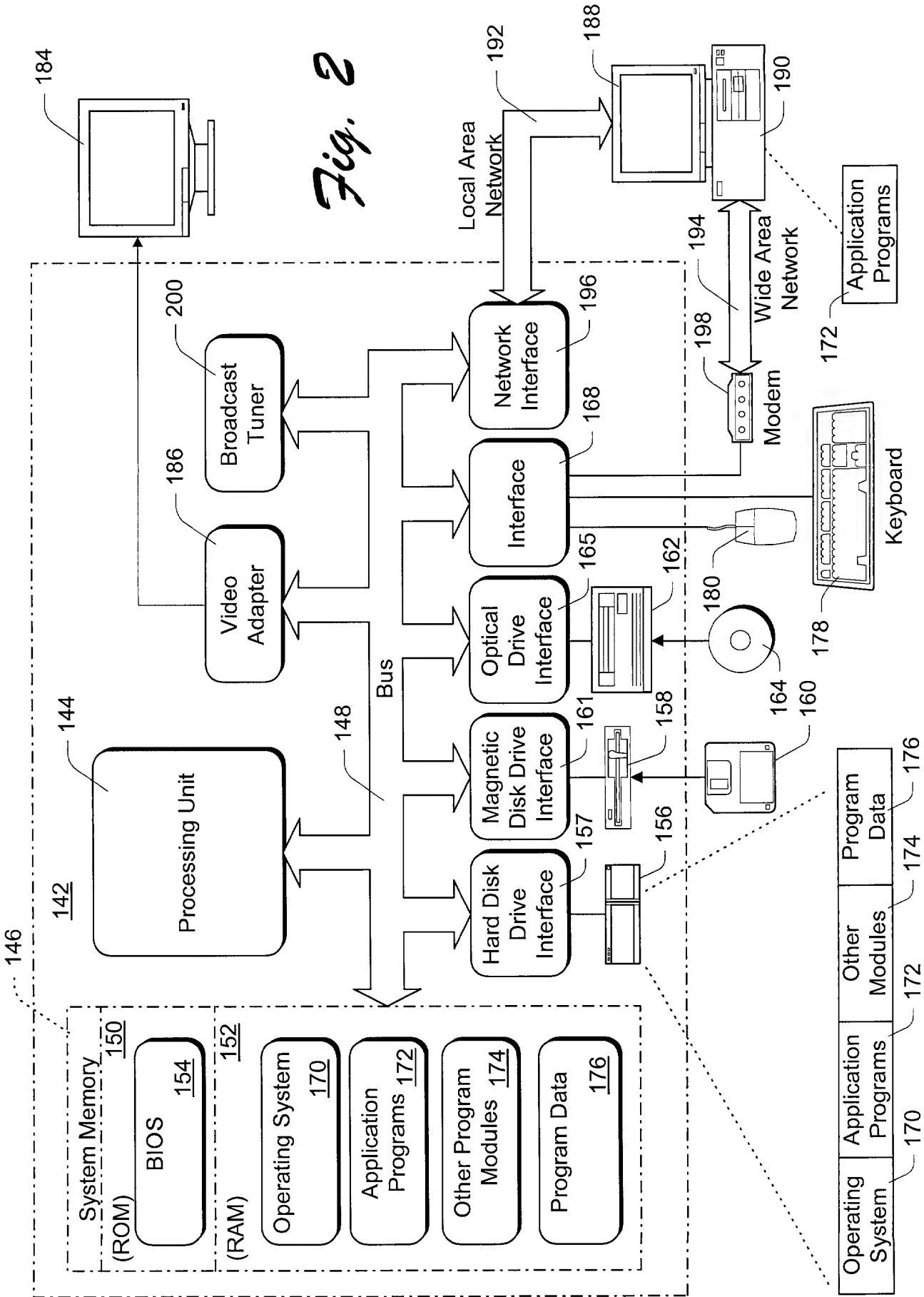


Fig. 1

Fig. 2



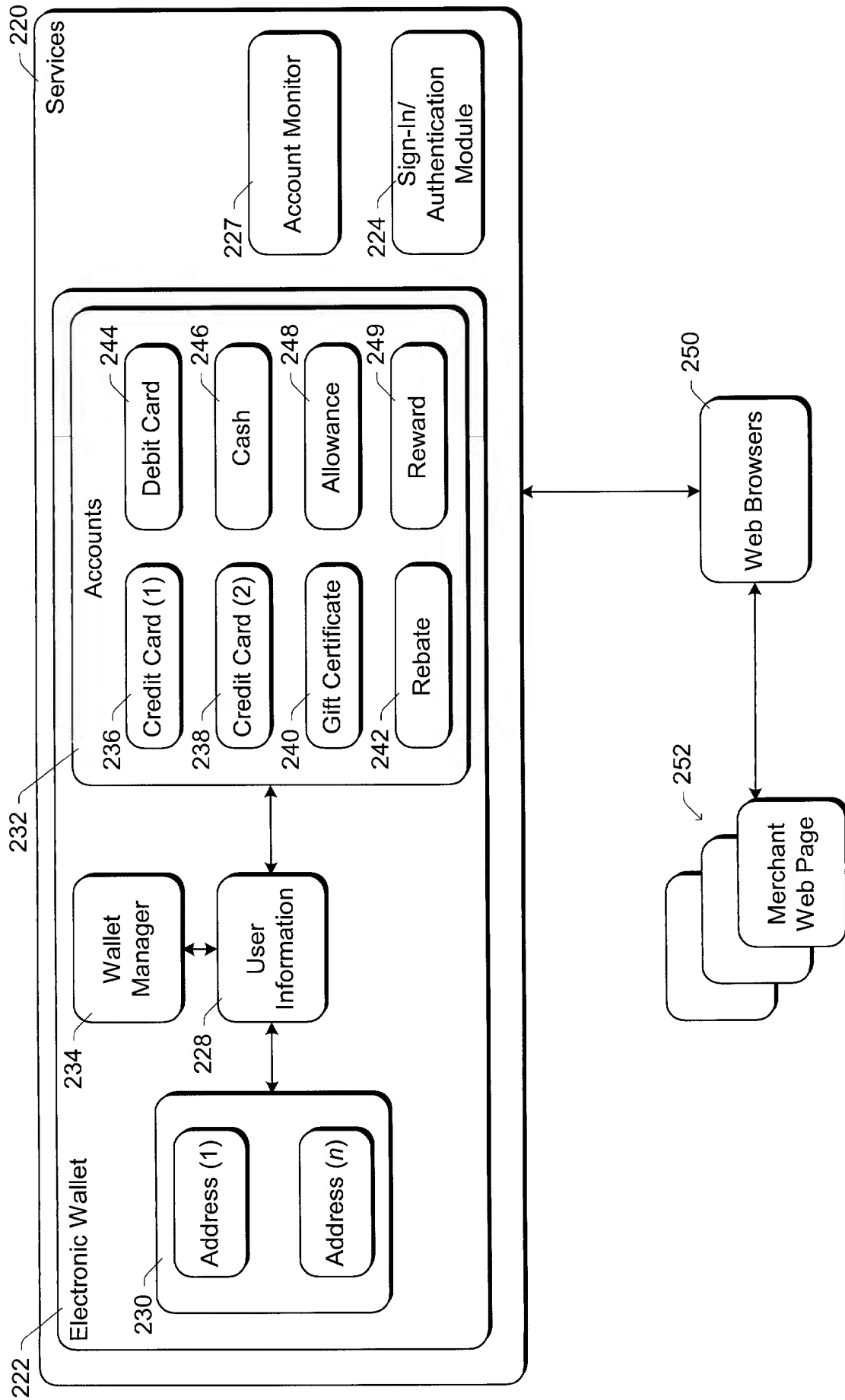


Fig. 3

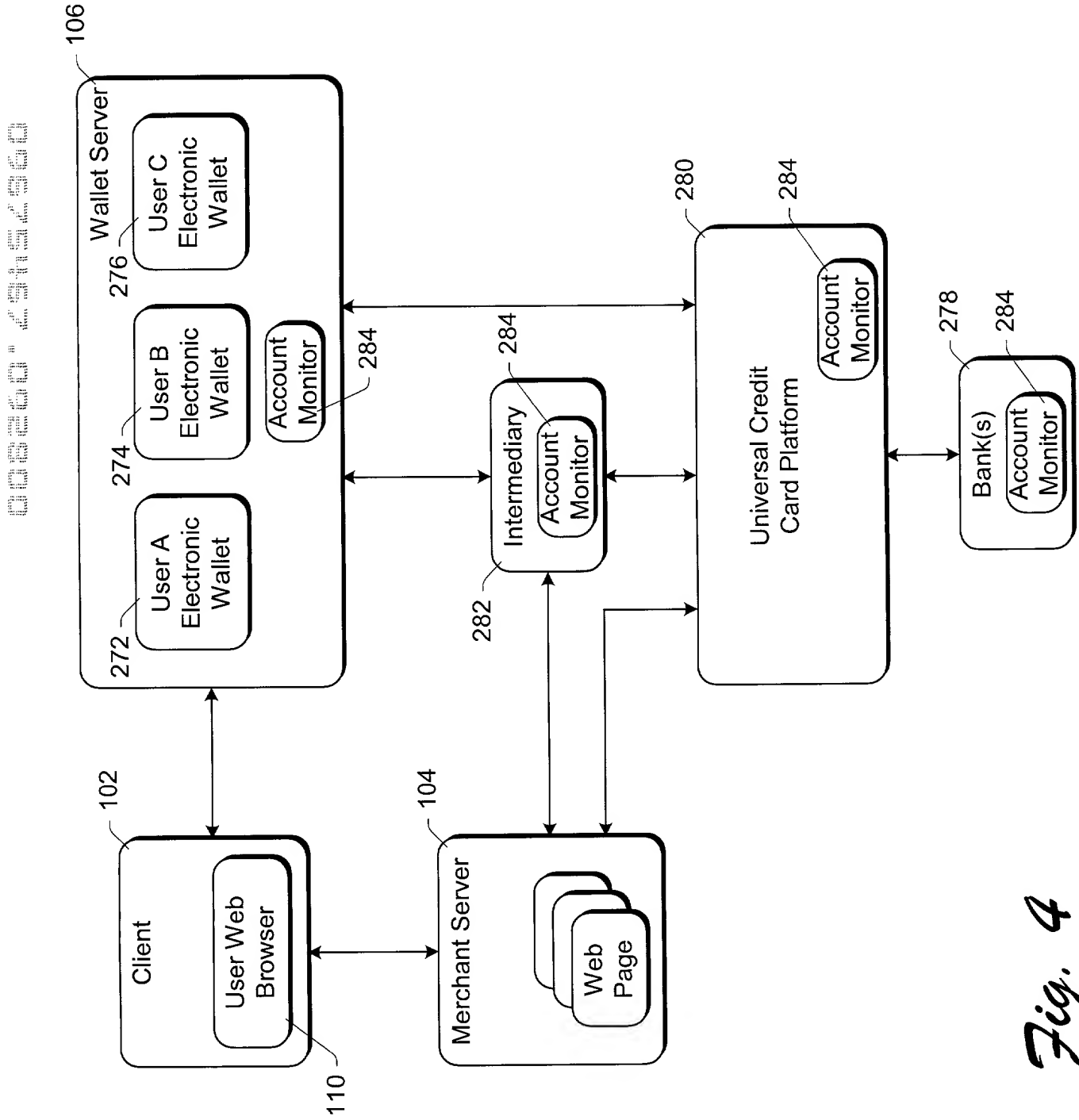


Fig. 4

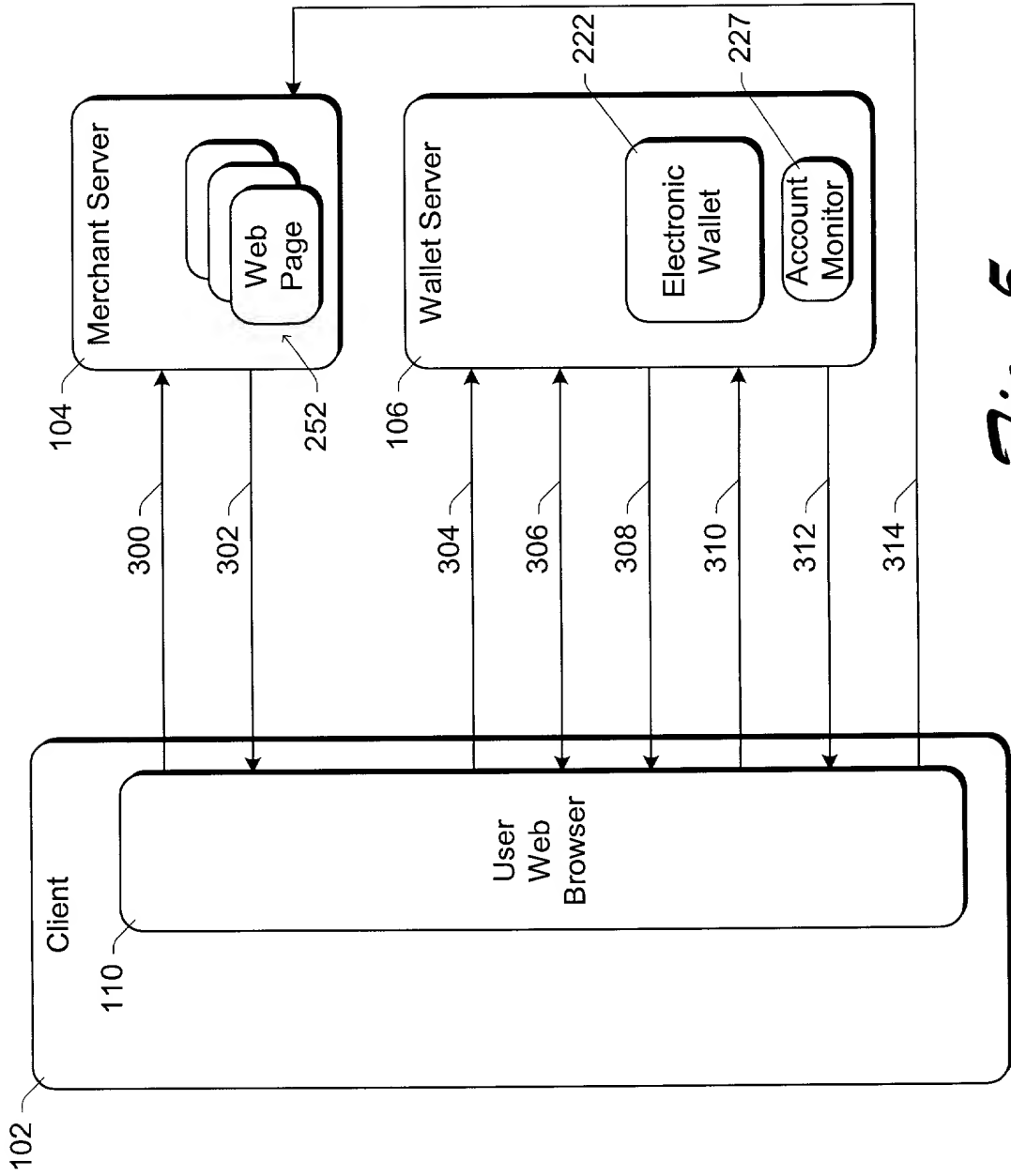


Fig. 5

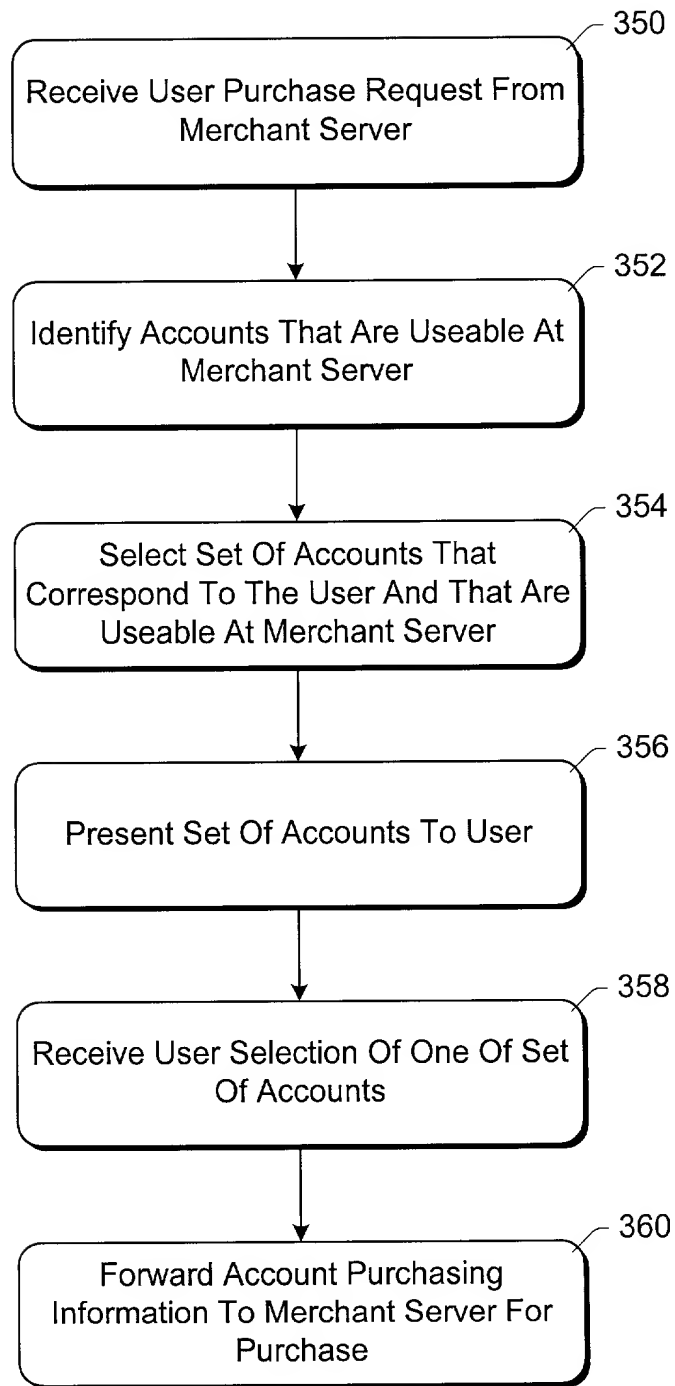


Fig. 6

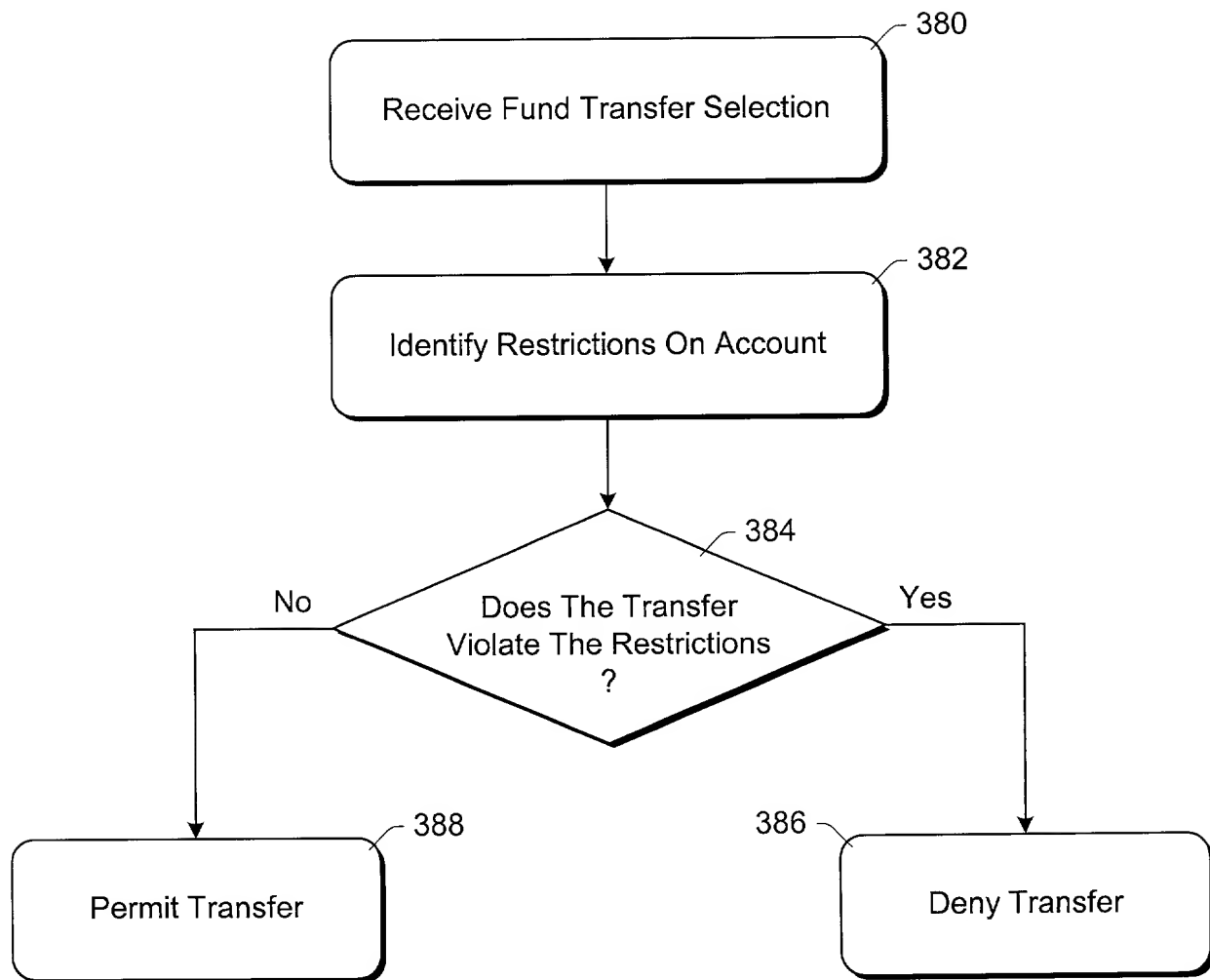
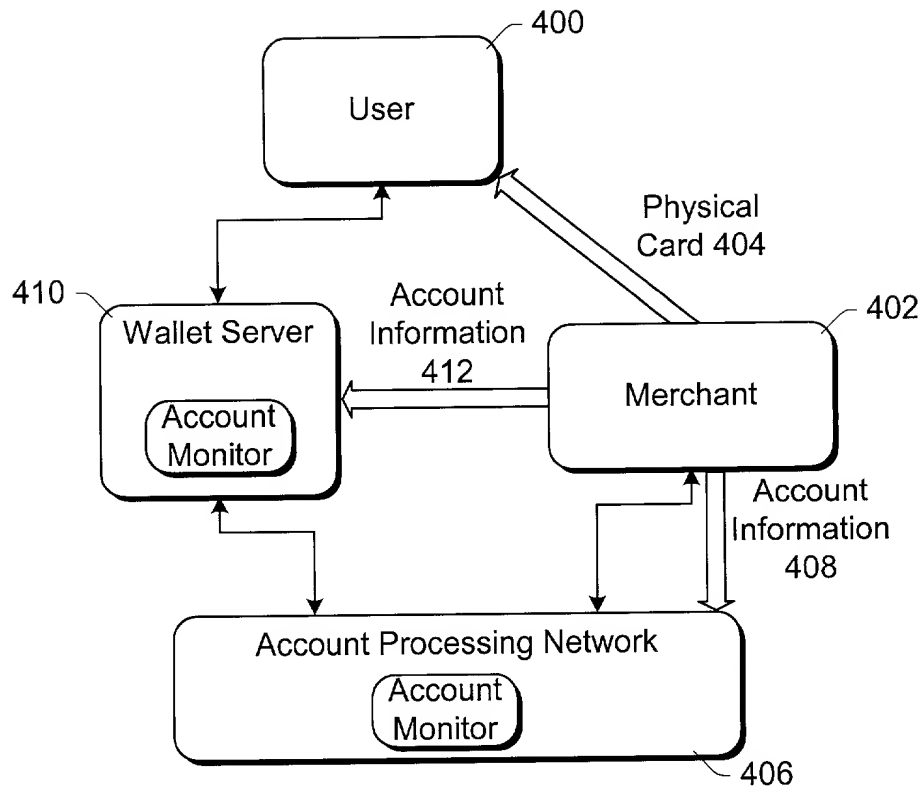


Fig. 7

*Fig. 8*

1 **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2 Inventorship Blinn et al.
 3 Applicant Microsoft Corporation
 4 Attorney's Docket No. MSI-624US
 Title: Method and System for Restricting the Usage of Payment Accounts

5 **DECLARATION FOR PATENT APPLICATION**

6 As a below named inventor, I hereby declare that:

7 My residence, post office address and citizenship are as stated below next to
 8 my name.

9 I believe I am the original, first and sole inventor (if only one name is listed
 10 below) or an original, first and joint inventor (if plural names are listed below) of the
 11 subject matter which is claimed and for which a patent is sought on the invention
 12 entitled "Method and System for Restricting the Usage of Payment Accounts," the
 specification of which is attached hereto.

13 I have reviewed and understand the content of the above-identified
 14 specification, including the claims.

15 I acknowledge the duty to disclose information which is material to the
 16 examination of this application in accordance with Title 37, Code of Federal
 17 Regulations, § 1.56(a).

18 **PRIOR FOREIGN APPLICATIONS:** no applications for foreign patents or
 19 inventor's certificates have been filed prior to the date of execution of this
 20 declaration.

21 **Power of Attorney**

22 I appoint the following attorneys to prosecute this application and transact all
 23 future business in the Patent and Trademark Office connected with this application:
 24 Lewis C. Lee, Reg. No. 34,656; Daniel L. Hayes, Reg. No. 34,618; Allan T.
 25

1 Sponseller, Reg. 38,318; Steven R. Sponseller, Reg. No. 39,384; James R.
2 Banowsky, Reg. No. 37,773; Lance R. Sadler, Reg. No. 38,605; Michael A. Proksch,
3 Reg. No. 43,021; Thomas A. Jolly, Reg. No. 39,241; David A. Morasch, Reg. No.
4 42,905; Kasey C. Christie, Reg. No. 40,559; Nathan R. Rieth, Reg. No. 44,302;
5 Brian G. Hart, Reg. No. 44,421; Katie E. Sako, Reg. No. 32,628 and Daniel D.
6 Crouse, Reg. No. 32,022.

7 Send correspondence to: LEE & HAYES, PLLC, 421 W. Riverside Avenue,
8 Suite 500, Spokane, Washington, 99201. Direct telephone calls to: Allan T.
9 Sponseller (509) 324-9256.

10
11 All statements made herein of my own knowledge are true and that all
12 statements made on information and belief are believed to be true; and further that
13 these statements were made with the knowledge that willful false statements and the
14 like so made are punishable by fine or imprisonment, or both, under Section 1001 of
15 Title 18 of the United States Code and that such willful false statement may
16 jeopardize the validity of the application or any patent issued therefrom.

17
18 * * * * *

19 Full name of inventor: Arnold N. Blinn

20 Inventor's Signature Arnold N. Blinn Date: 9/26/00

21 Residence: Clyde Hill, WA

22 Citizenship: USA

23 Post Office Address: 9401 NE 27th Street
24 Clyde Hill, WA 98004
25

Full name of inventor:

Joseph N. Coco

Inventor's Signature

Joseph N. Coco

Date: 9/26/2000

Residence:

Redmond, WA

Citizenship:

USA

Post Office Address:

15842 NE 83rd Ct.
Redmond, WA 98052